IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of:

Philip Hawkes et al..

Serial No.: 09/933,972

Filed: August 20, 2001

For: METHOD AND APPARATUS FOR SECURITY IN A DATA PROCESSING SYSTEM

Examiner: Michael Simitoski

Group Art Unit: 2134

Attorney Docket No.: 010497

ELECTRONIC FILING

Transmitted electronically to the Patent and Trademark Office.

Depositor's Name: *(type or print name)*

Date:

Signature:

BRIEF ON APPEAL

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Attention: Board of Patent Appeals and Interferences

Sirs:

This brief is submitted pursuant to 37 C.F.R. § 41.37 and in the format required by 37 C.F.R. § 41.37(c) and with the fee required by 37 C.F.R. § 41.20(b)(2).

1) REAL PARTY IN INTEREST

The real party in interest in the present pending appeal is Qualcomm, Inc., the assignee of the pending application as recorded at Reel 012128 Frame 0094 with the United States Patent and Trademark Office (Patent Office).

2) RELATED APPEALS AND INTERFERENCES

Neither Appellant, the Appellant's representative nor the Assignee are aware of any pending appeal or interference which would directly affect, be directly affected by, or have any bearing on the Board's decision in the present pending appeal.

3) STATUS OF THE CLAIMS

No claims were withdrawn.

No claims were canceled.

Claims 1-24 stand rejected.

No claims were allowed.

The rejection of claims 1-24 is being appealed.

4) STATUS OF AMENDMENTS

No proposed amendments were submitted after the current final rejection.

5) SUMMARY OF THE CLAIMED SUBJECT MATTER

With respect to independent claim 1 and referring to Figs. 1A-8D, the present invention is directed to a method for secure transmissions. (Figs. 7A-7D) The method of secure transmissions includes determining a registration key (RK) specific to a participant in a transmission. (RK in Figs. 4-6; Spec. p. 16, lines 1-5; Fig. 7B, 422). The method further includes determining a first key (BAK) and encrypting the first key (BAK) with the registration key (RK). (Fig. 7B, 426; Spec. p. 22, lines 22-23). The method further includes sending the encrypted first key (BAKI) to the participant in the transmission. (Fig. 7B, 428; Spec. p. 22, lines 23-24). The method further comprises determining a second key (SK) for decrypting content on a broadcast channel and encrypting the second key (SK) with the first key (BAK). (Fig. 4; Spec. p. 17, lines 23-25). The method further includes updating the first key (BAK) after a first time period has elapsed (Fig. 7B, 422, 424; Spec. p. 22, lines 18-28, 31-33) and updating the second key (SK) after a second time period has elapsed (Fig. 7C; Spec. p. 21, line 33-p. 22, line 5), wherein the second key (SK) is updated in two parts, a first part (BAK) known to the participant in the transmission and a second part (SKI) sent on the broadcast channel. (Spec. p. 18, line 24-p. 19, line 14).

With respect to independent claim 11 and referring to Figs. 1A-8D, the present invention is directed to a method for secure reception of a transmission. (Figs. 4-6). The method includes receiving a registration key (RK) specific to a participant in a transmission. (RK in Figs. 4-6; Spec. p. 16, lines 1-5; Fig. 7B, 422). The method further includes receiving a first key (BAK) encrypted with the registration key (RK) and decrypting the first key (BAK) with the registration

key (RK). (Fig. 4; Spec. p. 18, lines 5-17). The method further includes receiving a second key (SK) for decrypting content on a broadcast channel and decrypting the second key (SK) with the first key (BAK). (Fig. 4; Spec. p. 17, lines 23-25). The method further includes receiving a broadcast stream of information and decrypting the broadcast stream of information using the second key (SK). (Fig. 4; Spec. p. 15, lines 7-9; p. 17, lines 23-25). The method further includes receiving an updated first key (BAK) after a first time period has elapsed (Fig. 7B, 422, 424; Spec. p. 22, lines 18-28, 31-33) and receiving an updated second key (SK) after a second time period has elapsed (Fig. 7C; Spec. p. 21, line 33-p. 22, line 5), wherein the second key (SK) is updated in two parts, a first part (BAK) known to the participant in the transmission and a second part (SKI) sent on the broadcast channel. (Spec. p. 18, line 24-p. 19, line 14).

With respect to independent claim 15 and referring to Figs. 1A-8D, the present invention is directed to an infrastructure element in a wireless communication system (100) (Fig. 2) supporting a broadcast service option. (Fig. 2; Spec. p. 11, line 28-p. 12, line 21). The infrastructure element includes receive circuitry (304) adapted to receive a registration key (RK) specific to a participant in a transmission and to receive a first key (BAK) encrypted with the registration key (RK). (Fig. 4; Spec. p. 18, lines 5-17). The receive circuitry further adapted to, receive a second key (SK) for decrypting content on a broadcast channel encrypted with the first key (BAK), to receive an updated first key (BAK) after a first time period has elapsed, and to receive an updated second key (SK) after a second time period has elapsed (Fig. 7C; Spec. p. 21, line 33-p. 22, line 5), wherein the second key (SK) is updated in two parts, a first part (BAK) known to the participant in the transmission and a second part (SKI) sent on the broadcast

channel. (Spec. p. 18, line 24-p. 19, line 14). The infrastructure element further includes a user identification unit (308), operative to recover a short-time key for decrypting a broadcast message (Fig. 4; Spec. p. 16, lines 10-14), and includes a processing unit (316) operative to decrypt key information (Fig. 4; Spec. p. 18, lines 12-17), memory storage unit (314) for storing a registration key (RK) (Fig. 4; Spec. p. 14, lines 10-11), and a mobile equipment unit (ME) adapted to apply the short-time key for decrypting the broadcast message. (Fig. 4, Spec. p. 13, lines 29-30).

With respect to independent claim 22 and referring to Figs. 1A-8D, the present invention is directed to a wireless communication system (100). (Fig. 2). The system includes means for determining a registration key (RK) specific to a participant in a transmission. (RK in Figs. 4-6; Spec. p. 16, lines 1-5; Fig. 7B, 422). The system further includes means for determining a first key (BAK) and means for encrypting the first key (BAK) with the registration key (RK). (Fig. 7B, 426; Spec. p. 22, lines 22-23). The system further includes means for sending the encrypted first key (BAKI) to the participant in the transmission. (Fig. 7B, 428; Spec. p. 22, lines 23-24). The system further comprises means for determining a second key (SK) for decrypting content on a broadcast channel and means for encrypting the second key (SK) with the first key (BAK). (Fig. 4; Spec. p. 17, lines 23-25). The system further includes means for updating the first key (BAK) after a first time period has elapsed (Fig. 7B, 422, 424; Spec. p. 22, lines 18-28, 31-33) and means for updating the second key (SK) after a second time period has elapsed (Fig. 7C; Spec. p. 21, line 33-p. 22, line 5), wherein the second key (SK) is updated in two parts, a first part (BAK) known to the participant in the transmission and a second part (SKI) sent on the

broadcast channel. (Spec. p. 18, line 24-p. 19, line 14).

With respect to independent claim 23 and referring to Figs. 1A-8D, the present invention is directed to an infrastructure element (300). The infrastructure element includes a means for receiving a registration key (RK) specific to a participant in a transmission. (RK in Figs. 4-6; Spec. p. 16, lines 1-5; Fig. 7B, 422). The infrastructure element further includes a means for receiving a first key (BAK) encrypted with the registration key (RK) and means for decrypting the first key (BAK) with the registration key (RK). (Fig. 4; Spec. p. 18, lines 5-17). The infrastructure element further includes means for receiving a second key (SK) for decrypting content on a broadcast channel and means for decrypting the second key (SK) with the first key (BAK). (Fig. 4; Spec. p. 17, lines 23-25). The infrastructure element further includes means for receiving a broadcast stream of information and means for decrypting the broadcast stream of information using the second key (SK). (Fig. 4; Spec. p. 15, lines 7-9; p. 17, lines 23-25). The infrastructure element further includes means for updating a first key (BAK) after a first time period has elapsed (Fig. 7B, 422, 424; Spec. p. 22, lines 18-28, 31-33) and means for updating a second key (SK) after a second time period has elapsed (Fig. 7C; Spec. p. 21, line 33-p. 22, line 5), wherein the second key (SK) is updated in two parts, a first part (BAK) known to the participant in the transmission and a second part (SKI) sent on the broadcast channel. (Spec. p. 18, line 24-p. 19, line 14).

With respect to independent claim 24 and referring to Figs. 1A-8D, the present invention is directed to a digital storage device. (Spec. p. 26, lines 19-30). The digital storage device includes a first set of instructions for receiving a registration key (RK) specific to a participant in

a transmission. (RK in Figs. 4-6; Spec. p. 16, lines 1-5; Fig. 7B, 422). The digital storage device further includes a second set of instructions for receiving a first key (BAK) encrypted with the registration key (RK) and a third set of instructions for decrypting the first key (BAK) with the registration key (RK). (Fig. 4; Spec. p. 18, lines 5-17). The digital storage device further includes a fourth set of instructions for receiving a second key (SK) for decrypting content on a broadcast channel and a fifth set of instructions for decrypting the second key (SK) with the first key (BAK). (Fig. 4; Spec. p. 17, lines 23-25). The digital storage device further includes a sixth set of instructions for receiving a broadcast stream of information and a seventh set of instructions for decrypting the broadcast stream of information using the second key (SK). (Fig. 4; Spec. p. 15, lines 7-9; p. 17, lines 23-25). The digital storage device further includes an eight set of instructions for updating a first key (BAK) after a first time period has elapsed (Fig. 7B, 422, 424; Spec. p. 22, lines 18-28, 31-33) and for updating a second key (SK) after a second time period has elapsed (Fig. 7C; Spec. p. 21, line 33-p. 22, line 5), wherein the second key (SK) is updated in two parts, a first part (BAK) known to the participant in the transmission and a second part (SKI) sent on the broadcast channel. (Spec. p. 18, line 24-p. 19, line 14).

6) GROUNDS OF REJECTION TO BE REVIEWED

A. Whether claims 1-5, 10-11, 13-16 and 18-24 are unpatentable under 35 U.S.C. § 102 as being anticipated by U.S. Patent No. 6,690,795 to Richards et al. ("Richards").

B. Whether claim 6 is obvious under 35 U.S.C. § 103(a) over Richards in view of "FOLDOC, Free On-Line Dictionary Of Computing" by LinuxGuruz ("LinuxGuruz").

C. Whether claims 7-9 are obvious under 35 U.S.C. § 103(a) over Richards, as applied to claim 3, in further view of Applied Cryptography, Second Edition by Schneier ("Schneier").

D. Whether claims 12 and 17 are obvious under 35 U.S.C. § 103(a) over Richards, as applied to claims 11 and 15, in further view of U.S. Patent No. 6,073,122 to Wool ("Wool").

7) ARGUMENT

A. Claims 1-5, 10-11, 13-16 and 18-24 stand rejected under 35 U.S.C. § 102(b) as being unpatentable over Richards. Appellant respectfully traverses this rejection, as hereinafter set forth.

A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. *Verdegaal Brothers v. Union Oil Co. of California*, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). The identical invention must be shown in as complete detail as is contained in the claim. *Richardson v. Suzuki Motor Co.*, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989).

Appellant asserts that Richards does not and cannot anticipate under 35 U.S.C. § 102 the presently claimed invention of independent claim 1 and claims 2-5 depending therefrom, independent claim 11 and claims 13 and 14 depending therefrom, independent claim 15 and claims 16 and 18-21 depending therefrom and independent claims 22-24 because Richards does not describe, either expressly or inherently, the identical inventions in as complete detail as are contained in the claims. Specifically, Appellant's independent claims 1, 11, 15 and 22-24 each recite, in part, "***a*** second ***key for decrypting content*** on a broadcast channel".

The Final Office Action alleges:

> Regarding claims 1-5, 11, 13-14 & 22-24, Richards discloses
> [(1)] determining a registration key/UEV specific to a participant/set top box in a transmission (Fig. 26, #130&col. 20, lines 61-67),
> [(2)] determining ***a first key/CCK_1*** (Fig. 26, #133),
> [(3)] encrypting the first key/CCK_1 with the registration key (Fig. 26, #133),
> [(4)] determining ***a second key/PK and SK for decrypting content on a broadcast channel*** (Fig. 26, #159),
> [(5)] ***encrypting the second key with the first key ([PK]CCK_1, [SK]PK)***

[(6)] updating the first key/CCK after a first time period has elapsed (Fig. 23) and
[(7)] updating the ***second key/SK and PK*** after a second time period has elapsed, ***wherein the second key is updated in two parts (SK and PK), the first part/PK known to the participant in the transaction and a second part/SK sen[t] on a broadcast channel***(Fig. 26). (Final Office Action, pp. 4-5; emphasis added.)

Appellant respectfully disagrees with the mischaracterization of the disclosure of Richards and the continual reinterpretation of the disclosure of the reference throughout the analysis. Generally in the above-allegation of the Final Office Action, the Examiner, in (2), equates Appellant's "first key" to Richards' "CCK_1." Then the Examiner, in (4), equates Appellant's "**a** second **key**" to a **pair** of Richards' independent **keys** "PK and SK." Then the Examiner, in (5), states that Appellant's element of "encrypting the second key with the first key" is anticipated by Richards' disclosure of "[PK]CCK_1,[SK]PK". (Note: the term [PK]CCK_1,[SK]PK in Richards is read as PK encrypted by CCK_1 and SK encrypted by PK; Richards, col. 6, lines 30-38). Accordingly in (5), Richards' alleged "second key" which was defined in (4) as "PK and SK" are **not** both encrypted by the alleged "first key" of "CCK_1." Therefore, the Final Office Action's analysis is incomprehensible and therefore the finality is procedurally improper.

By way of substantive analysis, as stated, Appellant's invention as claimed in each independent claim recites, in part, "**a** second **key for decrypting content**" and **not,** as alleged in the Final Office Action, "a **pair** of keys (Richards' SK and PK) for decrypting content". Additionally, the alleged **pair** of keys "SK and PK" in the Final Office Action does not, as a pair, "decrypt content" according to Appellant's invention as claimed. Specifically, Richards clearly discloses that one key (Richards' ***SK) decrypts content*** and the other one key (Richards'

PK) decrypts the key (Richards' SK) that decrypts the content. (Richards, col. 9, lines 14-15). Furthermore, Richards clearly discloses that the SK and PK keys are independent and incapable of the Examiner's construction of a "composite" second key comprising Richards' SK key and Richards' PK key since Richards clearly and unequivocally discloses that these SK and PK keys have different update periods. (Richards, Fig. 9, 21; Figs. 10-12, 15A, 16-23). Clearly, the alleged **pair** of keys, namely SK and PK, do not describe, either expressly or inherently, Appellant's claim element of "***a*** second ***key for decrypting content*** on a broadcast channel".

Furthermore, Appellant's invention as claimed in each independent claim recites, in part, "***the*** second ***key is updated in two parts***, a first part known to the participant in the transmission and a second part sent on the broadcast channel" and **not,** as alleged in the Final Office Action, as "a **pair** of keys (Richards' SK and PK)". Since the Richards' SK key is the only key disclosed in Richards that decrypts content, the Richards's SK key would need to be "updated in two parts" in order to anticipate under 35 U.S.C. §102 Appellant's invention as presently claimed. A precise reading of Richards discloses that the Richards' SK key is updated as a unitary key that is delivered securely by being encrypted by Richards' PK key. (Richards, col. 9, line 26, 60; col. 10, lines 11-12; col. 13, line 54; Figs. 8, 14, 26). Clearly, Richards' single, unitary SK key which is updated by with a new single unitary encrypted SK key does not describe, either expressly or inherently, Appellant's claim element of "***the*** second ***key is updated in two parts***, a first part known to the participant in the transmission and a second part sent on the broadcast channel".

Therefore, Appellant's independent claim 1 and claims 2-5 depending therefrom, independent claim 11 and claims 13 and 14 depending therefrom, independent claim 15 and claims 16 and 18-21 depending therefrom and independent claims 22-24, cannot be anticipated under 35 U.S.C. § 102 by Richards. Accordingly, such claims are allowable over the cited prior art and Appellant respectfully requests the Board reverse the rejections of independent claim 1 and claims 2-5 depending therefrom, independent claim 11 and claims 13 and 14 depending therefrom, independent claim 15 and claims 16 and 18-21 depending therefrom and independent claims 22-24.

B. Claim 6 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Richards in view of FOLDOC, Free On-Line Dictionary of Computing" by LinuxGuruz ("LinuxGuruz"). Appellant respectfully traverses this rejection, as hereinafter set forth.

The nonobviousness of independent claim 1 precludes a rejection of claim 6 which depends therefrom because a dependent claim is obvious only if the independent claim from which it depends is obvious. *See* In re Fine, 5 U.S.P.Q.2d 1596, 1600 (Fed. Cir. 1988), *see also* MPEP § 2143.03. Therefore, the Appellant requests that the Examiner withdraw the 35 U.S.C. § 103(a) obviousness rejection to claim 6 which depends from independent claim 1.

C. Claims 7-9 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Richards, as applied to claim 3, and further in view of Applied Crytography, Second Edition by Schneier ("Schneier"). This rejection is respectfully traversed.

The nonobviousness of independent claim 1 precludes a rejection of claims 7-9 which depend therefrom because a dependent claim is obvious only if the independent claim from which it depends is obvious. *See* In re Fine, 5 U.S.P.Q.2d 1596, 1600 (Fed. Cir. 1988), *see also* MPEP § 2143.03. Therefore, the Appellant requests that the Examiner withdraw the 35 U.S.C. § 103(a) obviousness rejection to claims 7-9 which depend from independent claim 1.

D. Claims 12 and 17 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Richards, as applied to claims 11 and 15, and further in view of U.S. Patent 6,073,122 to Wool ("Wool"). This rejection is respectfully traversed.

The nonobviousness of independent claims 11 and 15 preclude a rejection of claims 12 and 17 which respectively depend therefrom because a dependent claim is obvious only if the independent claim from which it depends is obvious. *See* In re Fine, 5 U.S.P.Q.2d 1596, 1600 (Fed. Cir. 1988), *see also* MPEP § 2143.03. Therefore, the Appellant requests that the Examiner withdraw the 35 U.S.C. § 103(a) obviousness rejections to claims 12 and 17 which respectively depend from independent claims 11 and 15.

8) CLAIMS APPENDIX

A copy of claims 1-24 is appended hereto as Appendix A. Claims 1-24 are involved in the Appeal.

9) EVIDENCE APPENDIX

There is no evidence appendix.

10) RELATED APPEALS APPENDIX

There is no related appeals appendix.

CONCLUSION

Appellant respectfully submits that claims 1-24 are allowable. Appellant respectfully requests the reversal of the rejections of currently pending claims 1-24 for the reasons set forth above.

Respectfully submitted,

Dated: August 29, 2007

By: /Won Tae C. Kim/

Won Tae C. Kim, Reg. No. 40,457

QUALCOMM Incorporated
5775 Morehouse Drive
San Diego, California 92121
Telephone: (858) 651-6295
Facsimile: (858) 658-2502

APPENDIX A

Claims Appendix

Claims 1-24

U.S. Patent Application No. 09/933,972

Filed August 20, 2001

1. A method for secure transmissions, the method comprising:

determining a registration key specific to a participant in a transmission;

determining a first key;

encrypting the first key with the registration key;

sending the encrypted first key to the participant in the transmission;

determining a second key for decrypting content on a broadcast channel;

encrypting the second key with the first key;

updating the first key after a first time period has elapsed; and

updating the second key after a second time period has elapsed, wherein the second key is updated in two parts, a first part known to the participant in the transmission and a second part sent on the broadcast channel.

2. The method as in claim 1, wherein updating further comprises:

updating the first key according to a first time period; and

updating the second key according to a second time period, wherein the second time period is less than the first time period.

3. The method as in claim 2, wherein updating further comprises:

encrypting an updated first key with the registration key ; and

encrypting an updated second key with the updated first key.

4. The method as in claim 2, further comprising:

encrypting a broadcast stream of information using the second key; and

transmitting the encrypted broadcast stream of information.

5. The method as in claim 4, wherein the broadcast stream of information comprises video information.

6. The method as in claim 4, wherein the broadcast stream of information comprises Internet Protocol packets.

7. The method as in claim 3, further comprising:

calculating a registration key information message; and

transmitting the registration key information message.

8. The method as in claim 7, further comprising:

calculating a first key information message corresponding to the updated and encrypted first key; and

transmitting the first key information message.

9. The method as in claim 8, further comprising:

calculating a second key information message corresponding to the updated and encrypted second key; and

transmitting the second key information message.

10. The method as in claim 1, further comprising:

transmitting the encrypted first key; and

transmitting the encrypted second key.

11. A method for secure reception of a transmission, the method comprising:

receiving a registration key specific to a participant in a transmission;

receiving a first key encrypted with the registration key;

decrypting the first key with the registration key;

receiving a second key for decrypting content on a broadcast channel;

decrypting the second key with the first key;

receiving a broadcast stream of information; and

decrypting the broadcast stream of information using the second key;

receiving an updated first key after a first time period has elapsed; and

receiving an updated second key after a second time period has elapsed, wherein the second key is updated in two parts, a first part known to the participant in the transmission and a second part sent on the broadcast channel.

12. The method as in claim 11, further comprising:

storing the first key in a secure memory storage unit; and

storing the second key in a memory storage unit.

13. The method as in claim 11, further comprising:

recovering the first key from a first key information message; and

recovering the second key from a second key information message.

14. The method as in claim 11, further comprising:

updating the first key according to a first time period; and

updating the second key according to a second time period.

15. In a wireless communication system supporting a broadcast service option, an infrastructure element comprising:

a receive circuitry adapted to receive a registration key specific to a participant in a transmission, receive a first key encrypted with the registration key, receiving a second key for decrypting content on a broadcast channel encrypted with the first key, receiving an updated first key after a first time period has elapsed, and receiving an updated second key after a second time period has elapsed, wherein the second key is updated in two parts, a first part known to the participant in the transmission and a second part sent on the broadcast channel;

a user identification unit, operative to recover a short-time key for decrypting a broadcast message, comprising:

processing unit operative to decrypt key information;

memory storage unit for storing a registration key; and

a mobile equipment unit adapted to apply the short-time key for decrypting the broadcast message.

16. The infrastructure element as in claim 15, wherein the short-time key is processed by the user identification unit and passed to the mobile equipment unit.

17. The infrastructure element as in claim 15, wherein the memory storage unit is a secure memory storage unit.

18. The infrastructure element as in claim 15, wherein the memory storage unit stores a broadcast access key, and wherein the processing unit decrypts the short-time key using the broadcast access key.

19. The infrastructure element as in claim 18, wherein the short-time key is updated at a first frequency.

20. The infrastructure element as in claim 19, wherein the broadcast access key is updated at a second frequency less than the first frequency.

21. The infrastructure element as in claim 15, wherein the broadcast service option is a video service.

22. A wireless communication system, comprising:

means for determining a registration key specific to a participant in a transmission;

means for determining a first key;

means for encrypting the first key with the registration key;

means for sending the encrypted first key to the participant in the transmission;

means for determining a second key for decrypting content on a broadcast channel;

means for encrypting the second key with the first key;

means for updating the first key after a first time period has elapsed; and

means for updating the second key after a second time period has elapsed, wherein the second key is updated in two parts, a first part known to the participant in the transmission and a second part sent on the broadcast channel.

23. An infrastructure element, comprising:

means for receiving a registration key specific to a participant in a transmission;

means for receiving a first key encrypted with the registration key;

means for decrypting the first key with the registration key;

means for receiving a second key for decrypting content on a broadcast channel;

means for decrypting the second key with the first key;

means for receiving a broadcast stream of information; and

means for decrypting the broadcast stream of information using the second key;

means for updating the first key after a first time period has elapsed; and

means for updating the second key after a second time period has elapsed, wherein the second key is updated in two parts, a first part known to the participant in the transmission and a second part sent on the broadcast channel.

24. A digital storage device, comprising:

first set of instructions for receiving a registration key specific to a participant in a transmission;

second set of instructions for receiving a first key encrypted with the registration key;

third set of instructions for decrypting the first key with the registration key;

fourth set of instructions for receiving a second key for decrypting content on a broadcast channel;

fifth set of instructions for decrypting the second key with the first key;

sixth set of instructions for receiving the broadcast stream of information; and

seventh set of instructions for decrypting the broadcast stream of information using the second key;

eighth set of instructions for updating the first key after a first time period has elapsed, updating the second key after a second time period has elapsed, wherein the second key is updated in two parts, a first part known to the participant in the transmission and a second part sent on a broadcast channel.